GMR Institute of Technology
An Autonomous Institute Affiliated to JNTU-GV | GMRIT Training Tomorrow's Engineers Today

GMR Institute of Technology

Department of Computer Science and Engineering

Title of the Term Paper	: **An obfuscation technique for malware detection and protection in sandboxing**
Name of the Student	: Sampathirao Sai Prasanth
JNTU No.	: 22341A05F6
Name of the Course	: B.Tech. (CSE) Section: C Semester: 5th
Academic Year	: 2024-2025
Supervisor Name	:Dr. P. Annan Naidu

ABSTRACT:

Sandboxing has grown very prominent as a technique for malware detection and prevention, but with the passage of time and its prominence, cybercriminals have evolved advanced techniques to bypass it. Advanced strains of malware now can easily detect whether they are running inside a sandbox environment and delay execution of their malicious code till they break out of this controlled environment. One of the most common sandbox evasion methods used by attackers is monitoring user input—or lack thereof—as an indication of a sandbox. Where real machines would show extensive user activity, such as moving the mouse or hitting keys, sandboxes provide very little or no activity at all, marking them for malware. In this paper, we introduce a new approach generating artificial user activity data to model the natural patterns of a real environment, therefore making it harder for malware to determine whether it is running on a sandboxed or non-sandboxed system. This generated data can be further obfuscated by an AI tool called Delphix, which compresses data and hides it but retains consistency across cloned environments, hence keeping it even further from malware detection. Coupling advances in these technologies with sandboxing technology holds great promise for better detection and analysis capabilities against advanced malware.

Keywords: Sandboxing**,** Malware Evasion**,** User Activity Simulation**,** AI-based Obfuscation**,** Malware Detection

References:

[1] **Egele, M., Scholte, T., Kirda, E., & Kruegel, C. (2008).** "A Survey on Automated Dynamic Malware Analysis Techniques and Tools." *ACM Computing Surveys (CSUR)*, 44(2), 1-42. doi:10.1145/2089125.2089126

[2] **Moser, A., Kruegel, C., & Kirda, E. (2007).** "Exploring Multiple Execution Paths for Malware Analysis." *Proceedings of the 2007 IEEE Symposium on Security and Privacy (SP 2007)*, 231-245. doi:10.1109/SP.2007.14

[3] **Gardiner, J., & Nagaraja, S. (2016).** "On the Security of Machine Learning in Malware C&C Detection: A Survey." *ACM Computing Surveys (CSUR)*, 49(3), 1-39. doi:10.1145/2996355.

[4] **Kirda, E., & Kruegel, C. (2006).** "Behavior-based Spyware Detection." *Proceedings of the 15th Conference on USENIX Security Symposium*, 261-278.

[5] **Raffetseder, T., Kruegel, C., & Kirda, E. (2007).** "Detecting System Emulators." *Proceedings of the 10th International Conference on Information Security (ISC 2007),* 1-18. doi:10.1007/978-3-540-73354-8_1

Term Paper Supervisor

Term Paper Coordinator

HOD-CSE